

1/10

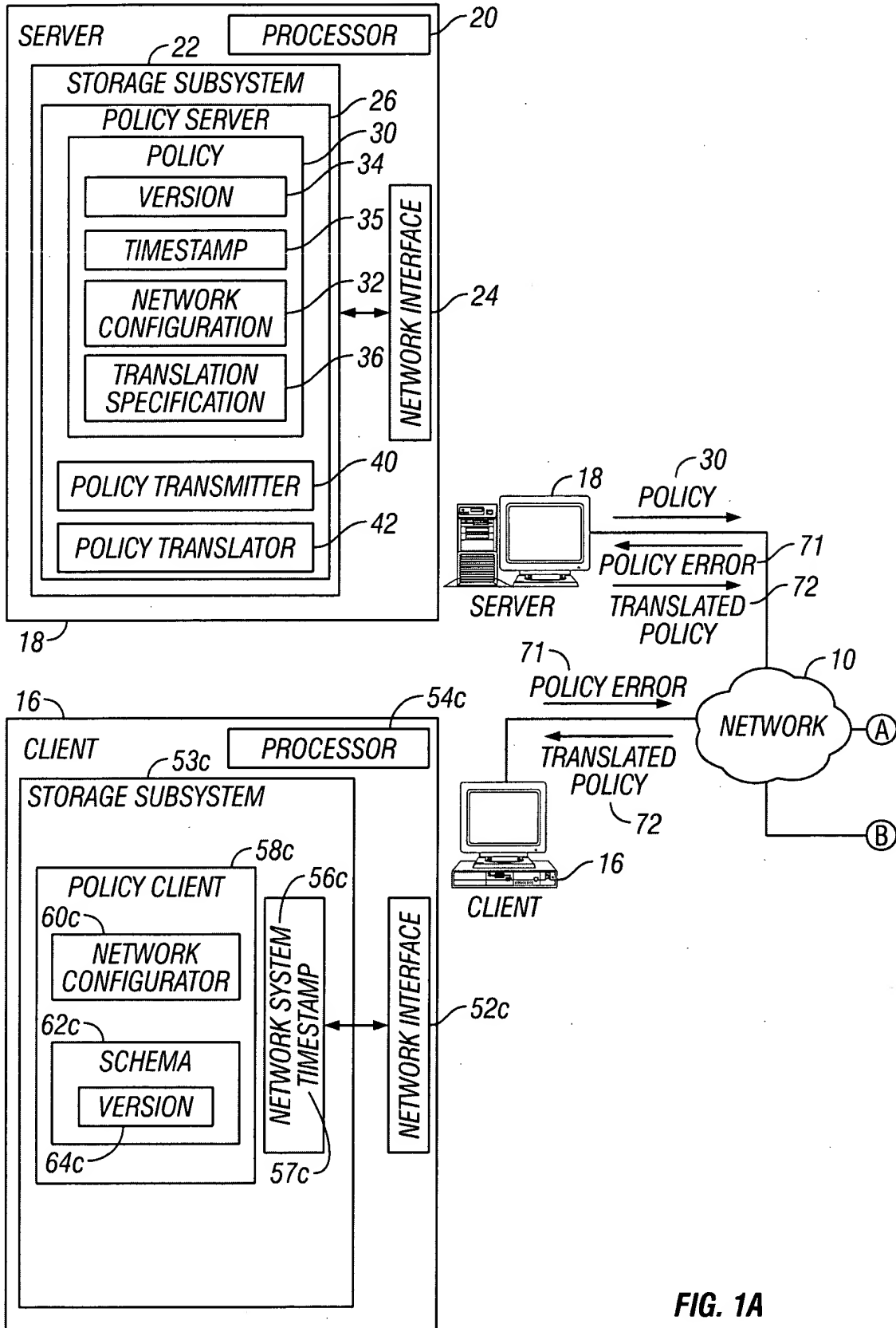
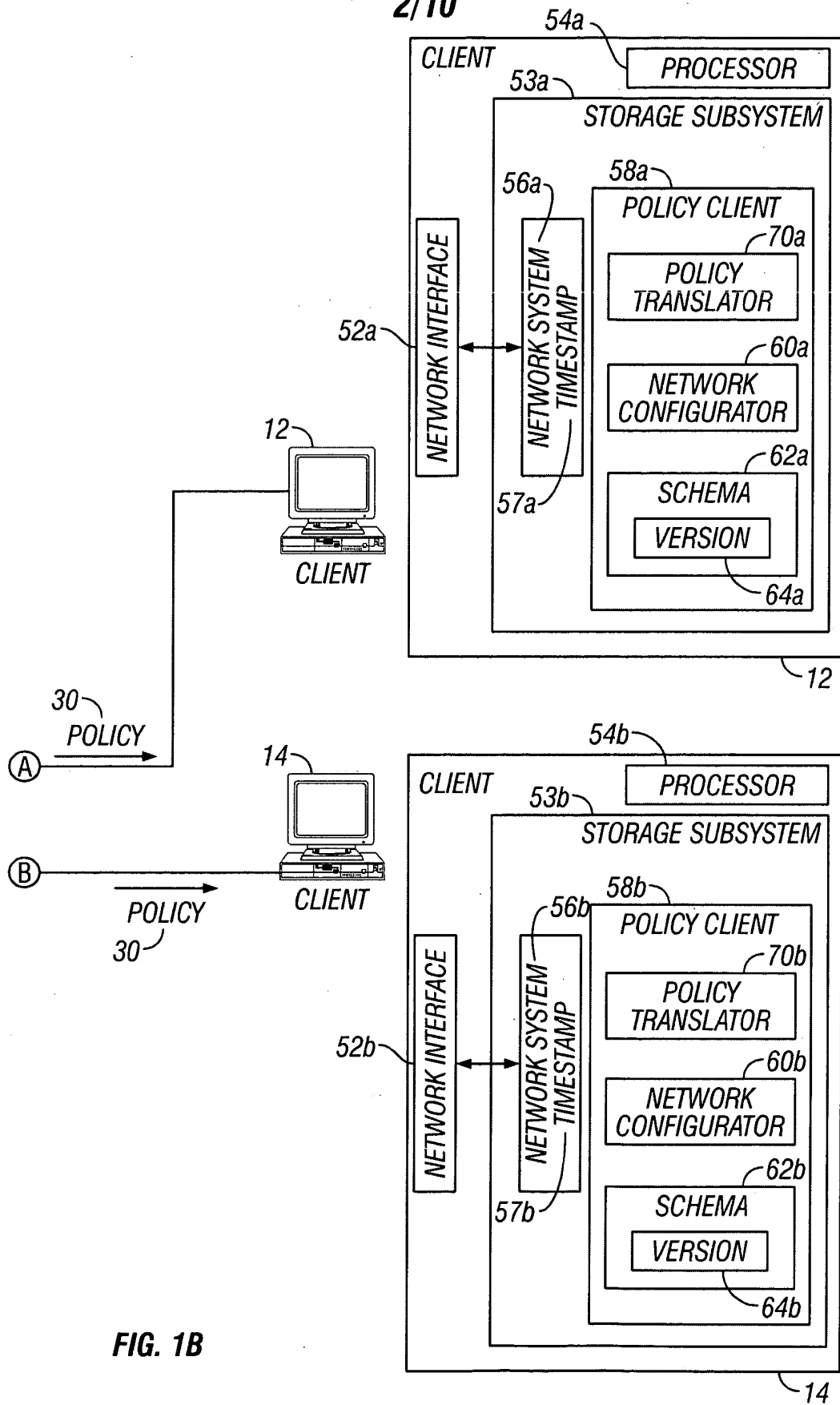


FIG. 1A

2/10



3/10

30

// Policy that conforms to the newer schema (specifies Rjindael):

<?xml version="1.0"?>

<DOCTYPE IPsecPolicyOnSystem PUBLIC "-//somestandard.org/IPsecPolicy/Version1.1"> 34

<IPsecPolicyOnSystem timestamp="2000-9-30_12:12:12"> 35

<IKEProposals>

90a ~<IKEProposal id="Proposal1" CipherAlgorithm="DES" HashAlgorithm="MD5" GroupId="DH768" AuthenticationMethod="Preshared"/> 92a

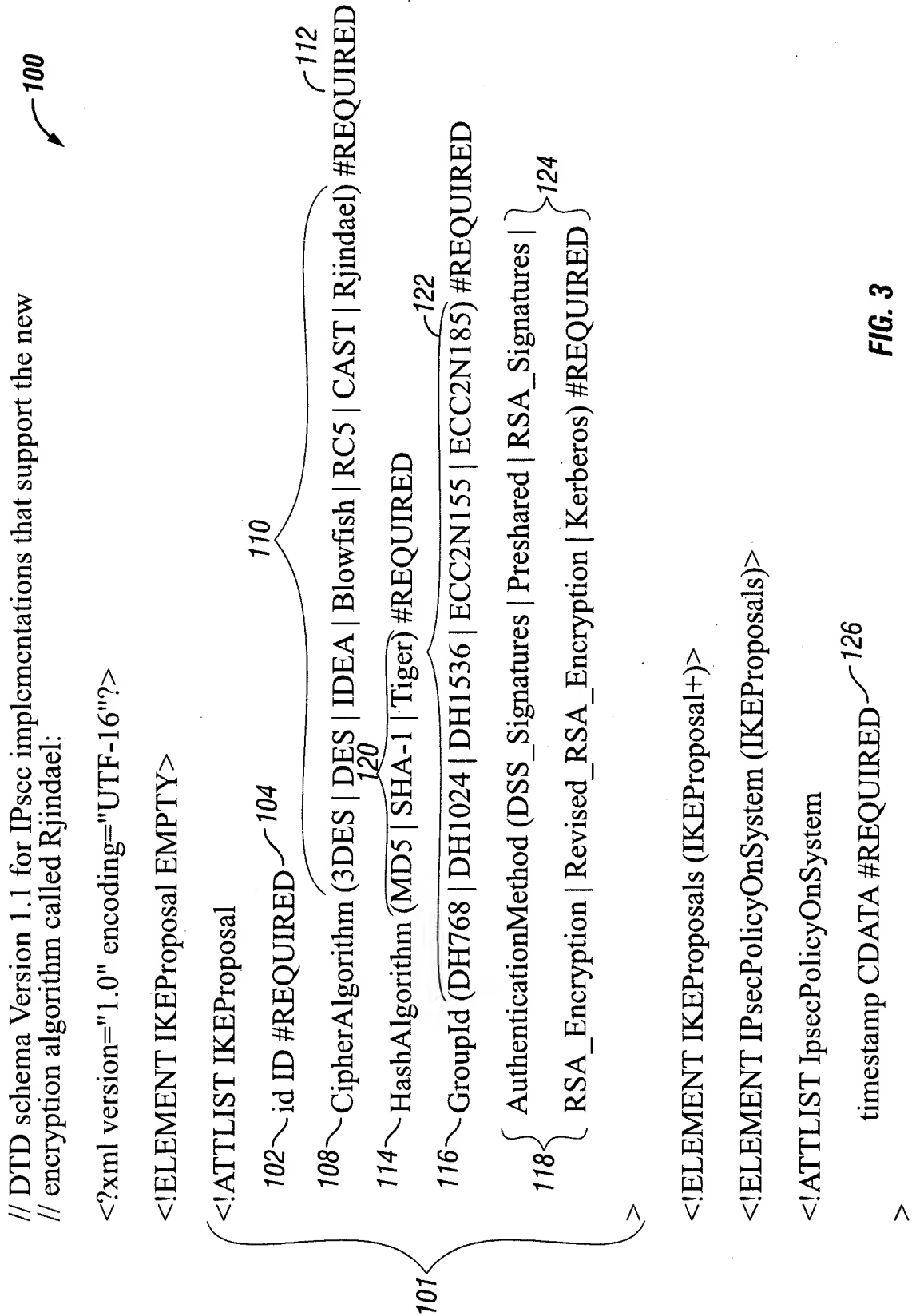
90b ~<IKEProposal id="Proposal2" CipherAlgorithm="Rjindael" HashAlgorithm="SHA-1" GroupId="DH1024" AuthenticationMethod="DSS_Signatures"/> 92b

</IKEProposals>

</IPsecPolicyOnSystem>

FIG. 2

4/10



5/10

// DTD schema for version 1.0 IPsec policy implementations (doesn't
 // include the new encryption algorithm called Rjindael):

<?xml version="1.0" encoding="UTF-16"?>

<!ELEMENT IKEProposal EMPTY>

<!ATTLIST IKEProposal

id ID #REQUIRED

132

CipherAlgorithm (3DES | DES | IDEA | Blowfish | RC5 | CAST) #REQUIRED

HashAlgorithm (MD5 | SHA-1 | Tiger) #REQUIRED

GroupId (DH768 | DH1024 | DH1536 | ECC2N155 | ECC2N185) #REQUIRED

AuthenticationMethod (DSS_Signatures | Preshared | RSA_Signatures |

RSA_Encryption | Revised_RSA_Encryption | Kerberos) #Required

>

<!ELEMENT IKEProposals (IKEProposal+)>

<!ELEMENT IPsecPolicyOnSystem (IKEProposals)>

<!ATTLIST IPsecPolicyOnSystem

timestamp CDATA #REQUIRED

>

FIG. 4

130

6/10

36

// XSLT file to transform the above policy into a policy conforming to the older
// schema. This transformation simply replaces attribute "Rjindael" with "3DES".

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- This stylesheet replaces the CipherAlgorithm Rjindael with 3DES, for IKE
implementations that do not support Rjindael. -->
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
  <xsl:output method="xml" version="1.0" encoding="UTF-8" indent="yes"/>

  <xsl:output doctype-public="//somestandard.org/IPsecPolicy/Version1.0"/> 146

    <xsl:template match="/*">
      <xsl:element name="IPsecPolicyOnSystem">
        <xsl:copy-of select="@*" />
        <xsl:element name="IKEProposals">
          <xsl:apply-templates select="IKEProposals" />
        </xsl:element>
      </xsl:element>
    </xsl:template>

    <xsl:template match="IKEProposals/IKEProposal">

      <xsl:element name="IKEProposal">
        <xsl:copy-of select="@*" />
        <xsl:if test="@CipherAlgorithm = 'Rjindael'"> 142a
          <xsl:attribute name="CipherAlgorithm">3DES</xsl:attribute> 142b
        </xsl:if>
      </xsl:element>
    </xsl:template>
  </xsl:stylesheet>
```

FIG. 5A

7/10

// Output resulting from applying the above transformation to the policy:

<?xml version="1.0" encoding="utf-8"?>

<!DOCTYPE IPsecPolicyOnSystem PUBLIC "-//somestandard.org/IPsecPolicy/Version1.0">

<IPsecPolicyOnSystem timestamp="2000-9-30 12:12:12">

<IKEProposals>

<IKEProposal id="Proposal1" CipherAlgorithm="DES" HashAlgorithm="MD5" GroupId="DH768" AuthenticationMethod="Preshared"/>

<IKEProposal id="Proposal2" CipherAlgorithm="3DES" HashAlgorithm="SHA-1" GroupId="DH1024" AuthenticationMethod="DSS_Signatures"/>

</IKEProposals>

</IPsecPolicyOnSystem>

FIG. 5B

8/10

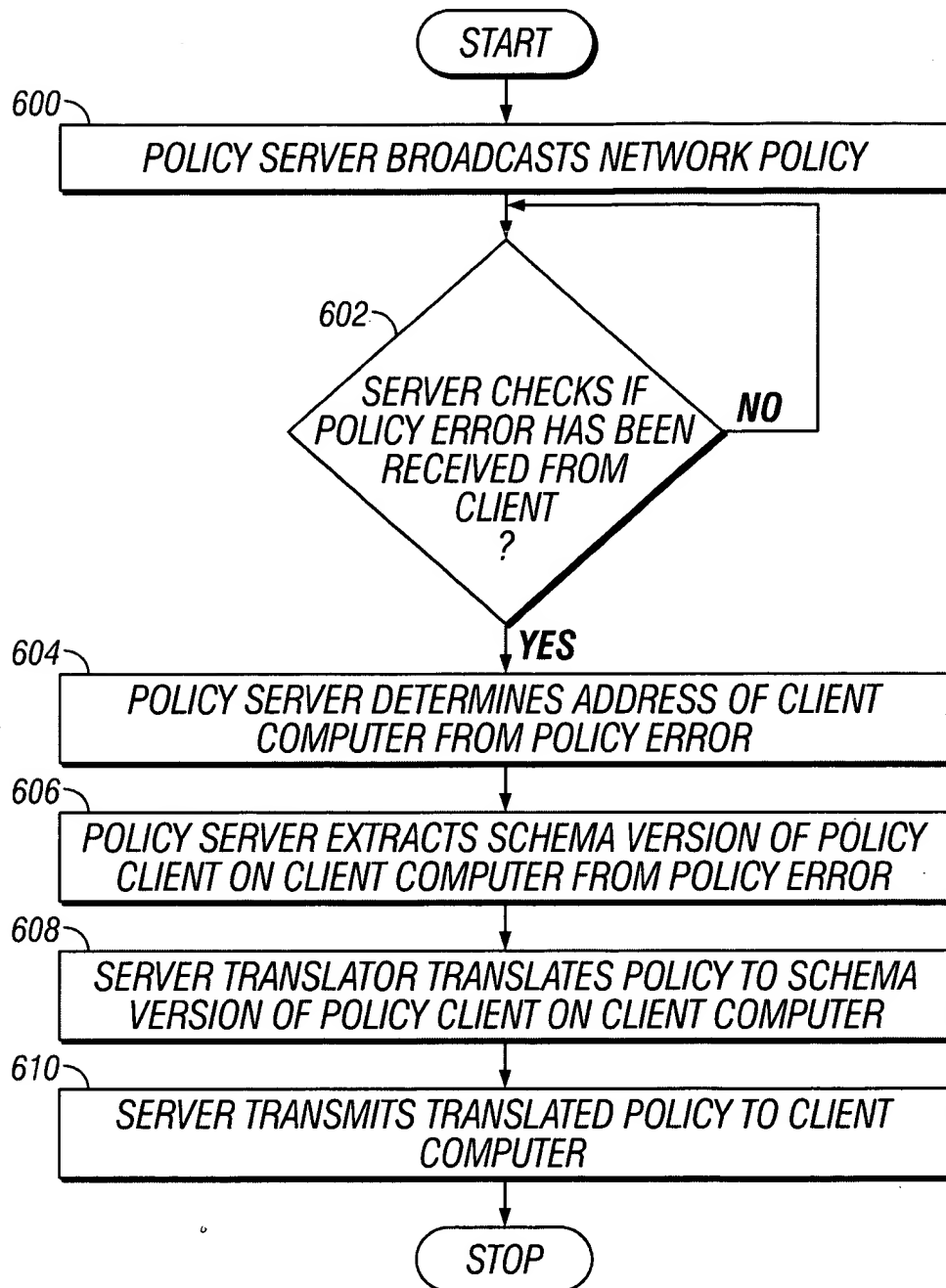


FIG. 6

9/10

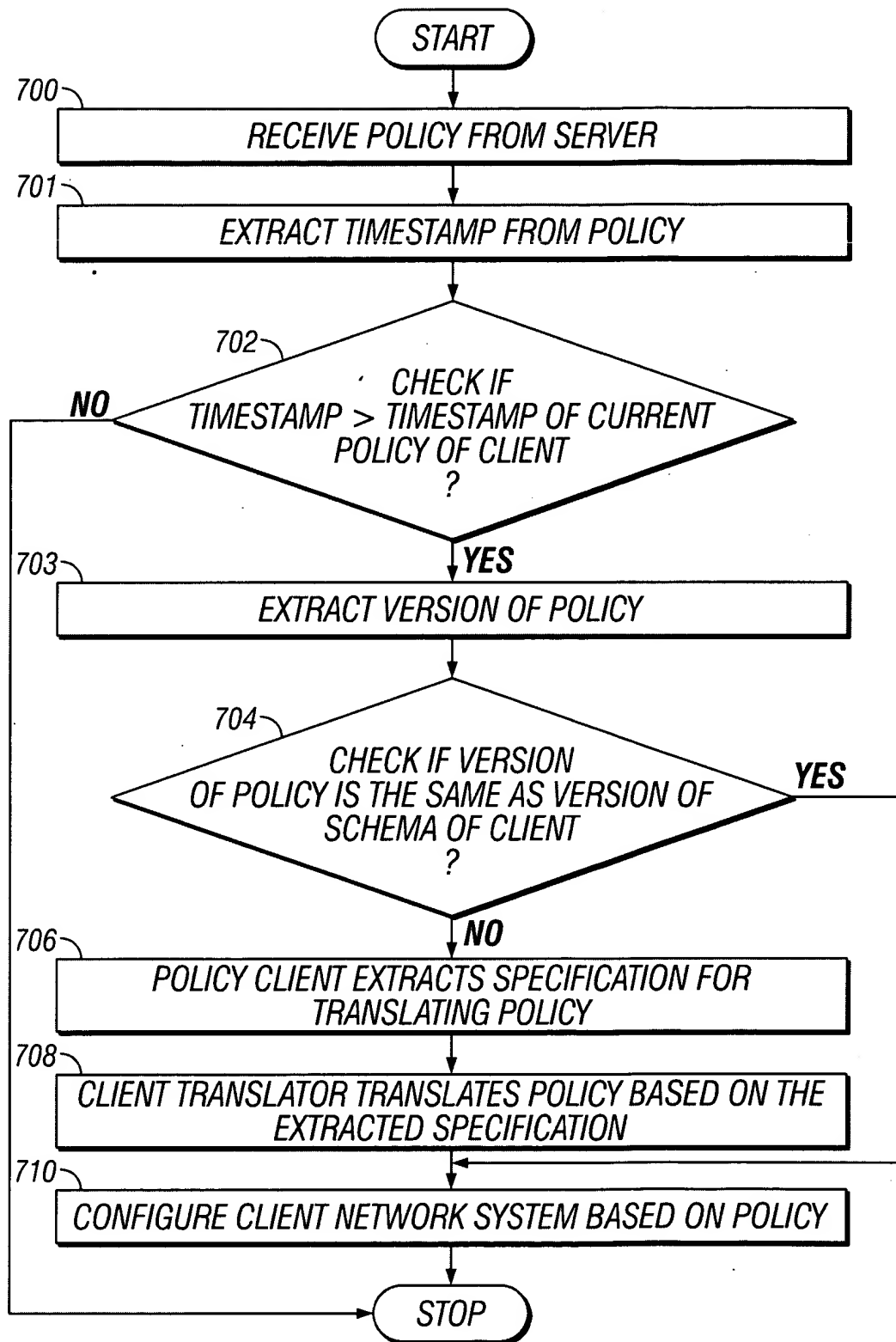


FIG. 7A

10/10

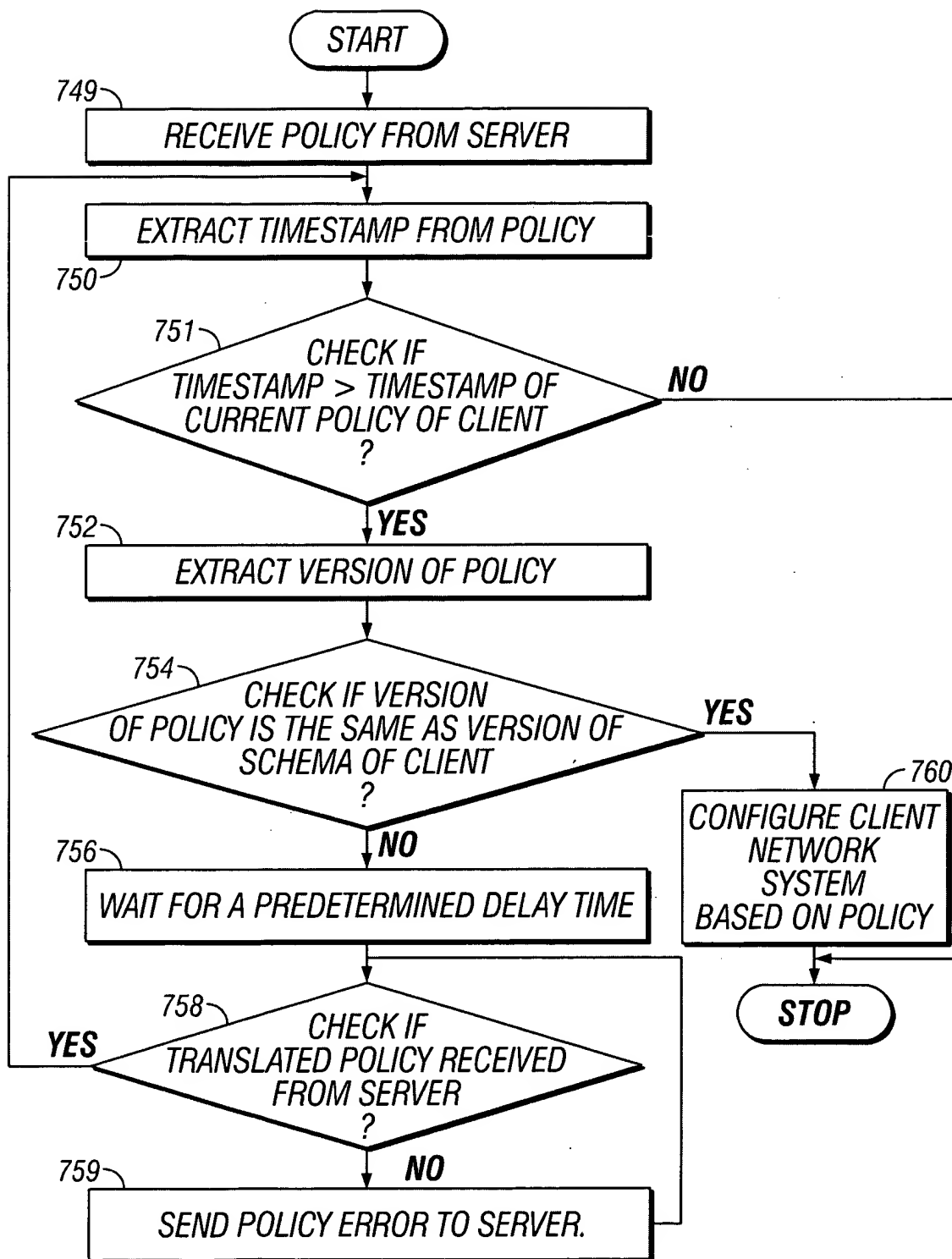


FIG. 7B